COMPANION TO THE NEXUS SECURE WEBSITE CHECKLIST

Website Security Scan Checklist

Free scanners turn website hardening into evidence you can show a customer, an insurer, or a board. Run them in this order, confirm each finding before you change anything, and fix what's real. Only scan sites you own or have written permission to test. Numbers in brackets refer to the sources on page 2.

1. Run the scanners

- [ ] **internet.nl** on the bare domain (example.com, not www): IPv6, DNSSEC, HTTPS and TLS, security headers, security.txt, route origin validation (RPKI). Target: 100%. [1]
- [ ] **Qualys SSL Labs**: certificate chain, protocols, cipher suites, and real-browser handshakes. Target: A+. [2]
- [ ] **MDN HTTP Observatory**: security headers and Content Security Policy (CSP), with suggested fixes. Target: A+, every test passing. [3]
- [ ] **Security Headers**: run on the bare domain with redirect-following off, to check the headers on the redirect itself. Target: A+. [4]
- [ ] **hstspreload.org**: eligibility check. Fix every error before submitting. [5]
- [ ] **A broad external scanner** (for example, Sitelemetry): exposed files (/.env, /.git), open cross-origin resource sharing (CORS), missing CAA records, server banners. Treat results as leads to confirm. [6]
- [ ] **Google CSP Evaluator** for your policy, and **crt.sh** for every certificate logged for your domain. [7]

2. Read the results

- [ ] Open one ticket per finding: evidence, fix, owner, retest date. Close it only after a rescan shows it fixed.
- [ ] Reproduce each finding with a second tool or a direct DNS or HTTP check before changing anything.
- [ ] Rule out common false positives: a "missing" CAA record on www when the bare domain has CAA records [8]; a default CDN banner such as Server: cloudflare [9].
- [ ] Check the report timestamp against your last deployment; some scanners cache results for several minutes.
- [ ] Record any accepted risk: the reason, who approved it, and when you'll revisit it.

3. Avoid the traps that cost points

- [ ] Add security headers to redirect-only hosts, which scanners still grade [1]. CDN-generated redirects skip your site's headers; use a CDN response-header rule [10] (CSP default-src 'none', X-Frame-Options DENY, Referrer-Policy). Mostly a scoring fix: little real protection on a redirect [11].
- [ ] For HSTS preload, send http://example.com to https://example.com first, then to www [5][12].
- [ ] Submit for preload only if you are committed to HTTPS on every current and future subdomain; removal takes months [5].
- [ ] Before turning on includeSubDomains, list every DNS record and give each web-facing host a valid certificate (watch old webmail and vendor CNAMEs); browsers give visitors no way past the error [13].
- [ ] Check live headers for host defaults, such as Access-Control-Allow-Origin: * added by some static hosts [9]; detach or override them [14].
- [ ] Decide on TLS 1.3-only deliberately: it clears cipher findings [15] but locks out TLS 1.2-only clients and some inspection proxies, and NIST still requires TLS 1.2 support for government systems [16]. Turn early data (0-RTT) off; it can be replayed [15].
- [ ] Before dropping 'unsafe-inline' from style-src, move every style= attribute and <style> block (including script-built HTML) into stylesheets [17]; add a CI check.
- [ ] Use Cross-Origin-Embedder-Policy credentialless where require-corp would break images or frames; leave it off pages with CAPTCHA or other third-party frames [18].
- [ ] List a Canonical URL in security.txt for every address it's served from, including the bare domain [19].

4. Keep it green

[ ]	Snapshot DNS and CDN security settings and compare them daily with a reviewed baseline; investigate any unexplained change.
[ ]	Make a failing check open a ticket or send an alert, so drift can't sit unnoticed.
[ ]	Compare live response headers with your intended configuration on a schedule.
[ ]	Rescan after every platform, hosting, or DNS change, and at least monthly; keep the reports as evidence.
[ ]	Give every new subdomain a valid certificate before it goes live.

Sources

[1] Internet.nl, Website test and test explanations. internet.nl
[2] Qualys, SSL Server Test. ssllabs.com/ssltest
[3] Mozilla, HTTP Observatory. developer.mozilla.org/en-US/observatory
[4] Security Headers report. securityheaders.com
[5] Chromium, HSTS Preload List Submission (requirements and removal). hstspreload.org
[6] Sitelemetry, website security audit. sitelemetry.com
[7] Google, CSP Evaluator (csp-evaluator.withgoogle.com); Sectigo, crt.sh (crt.sh)
[8] IETF RFC 8659, DNS Certification Authority Authorization (CAA), Section 3, 2019. rfc-editor.org/rfc/rfc8659
[9] Cloudflare, Serving Pages: default response headers. developers.cloudflare.com/pages/configuration/serving-pages
[10] Cloudflare, Response Header Transform Rules. developers.cloudflare.com/rules/transform/response-header-modification
[11] OWASP, HTTP Security Response Headers Cheat Sheet. cheatsheetseries.owasp.org
[12] Mozilla, Web Security Guidelines: HTTP redirections. infosec.mozilla.org/guidelines/web_security
[13] IETF RFC 6797, HTTP Strict Transport Security, Section 12.1, 2012. rfc-editor.org/rfc/rfc6797
[14] Cloudflare, Pages headers (_headers, detaching a header). developers.cloudflare.com/pages/configuration/headers
[15] IETF RFC 9846, TLS 1.3 (obsoletes RFC 8446), January 2026. rfc-editor.org/rfc/rfc9846
[16] NIST SP 800-52 Rev. 2, Guidelines for TLS Implementations, 2019 (under review in 2026). doi.org/10.6028/NIST.SP.800-52r2
[17] MDN Web Docs, CSP style-src directive. developer.mozilla.org
[18] MDN Web Docs, Cross-Origin-Embedder-Policy header. developer.mozilla.org
[19] IETF RFC 9116, security.txt, Section 2.5.2 (Canonical), 2022. rfc-editor.org/rfc/rfc9116
[20] OWASP Top 10:2025 (A02 Security Misconfiguration, A04 Cryptographic Failures). owasp.org/Top10/2025
[21] NIST CSWP 29, Cybersecurity Framework (CSF) 2.0, 2024: PR.PS, DE.CM. doi.org/10.6028/NIST.CSWP.29

Last reviewed November 16, 2026. General information, not a guarantee of security or compliance; confirm against the official sources. Tool names are trademarks of their owners; Nexus Security Advisors has no affiliation with them.

Full cited checklist: nexussecurityadvisors.com/secure-website. Want a second set of eyes? Request a consultation at nexussecurityadvisors.com/get-started.